

Full Disk Encryption Pre-Boot Authentication Reference

ZENworks® 11 Support Pack 2

July 2, 2012

Legal Notices

Novell, Inc., makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc., makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. See the [Novell International Trade Services Web page \(http://www.novell.com/info/exports/\)](http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Copyright © 2012 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

Novell, Inc.
1800 South Novell Place
Provo, UT 84606
U.S.A.
www.novell.com

Online Documentation: To access the latest online documentation for this and other Novell products, see the [Novell Documentation Web page \(http://www.novell.com/documentation\)](http://www.novell.com/documentation/).

Novell Trademarks

For Novell trademarks, see [the Novell Trademark and Service Mark list \(http://www.novell.com/company/legal/trademarks/tmlist.html\)](http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

All third-party trademarks are the property of their respective owners.

Contents

About This Guide	5
Part I Introduction	7
1 The ZENworks PBA	9
1.1 Security	9
1.2 Implementation	9
1.2.1 Standard Hard Disk	9
1.2.2 Self-Encrypting Hard Disk	10
1.3 Authentication Methods	10
1.3.1 User Capturing	10
1.3.2 Single Sign-On	10
2 The ZENworks PBA Boot Process	11
Part II PBA Management	13
3 Activating Pre-Boot Authentication	15
4 Enabling User Capturing	17
4.1 Using a ZENworks Control Center Quick Task	17
4.2 Using the Full Disk Encryption Agent	18
5 Manually Adding Users	21
5.1 Using a ZENworks Control Center Quick Task	21
5.2 Using the Full Disk Encryption Agent	22
6 Enabling Single Sign-On with Windows	25
6.1 Activating Single Sign-On in the Disk Encryption Policy	25
6.2 Configuring Windows Login	26
6.3 Using the Novell Client	27
7 Synchronizing PBA and Windows Credentials	29
7.1 Using the Windows Login	29
7.2 Using a ZENworks Control Center Quick Task	30
7.3 Using the Full Disk Encryption Agent	30

Part III PBA Override	33
8 PBA Override Versus Emergency Recovery	35
9 Using the ZENworks PBA Helpdesk for PBA Override (User)	37
10 Generating a Response Sequence for PBA Override (Administrator)	41
10.1 Assigning the Administrator Rights Needed for PBA Override.	41
10.2 Generating a Response with the Zone Key	43
10.3 Generating a Response with a PBA Override File.	44
11 Overriding the PBA with an ERI File	47

About This Guide

This *Novell ZENworks 11 Full Disk Encryption Pre-Boot Authentication Reference* provides information to help you understand, manage, and override ZENworks Pre-Boot Authentication. It is organized as follows:

- ♦ [Part I, "Introduction," on page 7](#)
- ♦ [Part II, "PBA Management," on page 13](#)
- ♦ [Part III, "PBA Override," on page 33](#)

Audience

This guide is written for the ZENworks Full Disk Encryption administrators.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation.

Additional Documentation

ZENworks Full Disk Encryption is supported by other documentation (in both PDF and HTML formats) that you can use to learn about and implement the product. For additional documentation, see the [ZENworks 11 documentation Web site \(http://www.novell.com/documentation/zenworks11\)](http://www.novell.com/documentation/zenworks11).

Introduction

The following sections introduce ZENworks Pre-Boot Authentication:

- ♦ [Chapter 1, “The ZENworks PBA,”](#) on page 9
- ♦ [Chapter 2, “The ZENworks PBA Boot Process,”](#) on page 11

1 The ZENworks PBA

Pre-boot authentication is the process of authenticating a user to a device before the device boots to the primary operating system. For ZENworks 11 Full Disk Encryption, the ZENworks Pre-Boot Authentication module, referred to as the *ZENworks PBA*, performs this operation on a device.

- ♦ [Section 1.1, “Security,” on page 9](#)
- ♦ [Section 1.2, “Implementation,” on page 9](#)
- ♦ [Section 1.3, “Authentication Methods,” on page 10](#)

1.1 Security

The ZENworks PBA is hosted by a fully functional Linux system installed on the device. At device startup, the Linux system boots and displays the ZENworks PBA login.

The primary advantage of the ZENworks PBA is increased security over the standard Windows login. The Linux system is hardened, meaning that it has been explicitly configured for security and reliability. The ZENworks PBA is protected against alteration through the use of MD5 checksums, and the ZENworks PBA applies strong encryption for the keys used in the authentication process.

With standard hard disks encrypted by ZENworks 11 Full Disk Encryption, the ZENworks PBA does not prevent intruders from seeing the encrypted partitions. However, because the partitions are encrypted, none of the data is accessible until ZENworks PBA login is successful.

With self-encrypting hard disks, the ZENworks PBA prevents intruders from seeing the disks. The disks remain hidden and locked until ZENworks PBA login is successful.

1.2 Implementation

The ZENworks PBA implementation differs for a standard hard disk and a self-encrypting hard disk.

- ♦ [Section 1.2.1, “Standard Hard Disk,” on page 9](#)
- ♦ [Section 1.2.2, “Self-Encrypting Hard Disk,” on page 10](#)

1.2.1 Standard Hard Disk

A standard hard disk is an IDE, SATA, or PATA disk that is not self-encrypting and therefore can be encrypted by ZENworks 11 Full Disk Encryption.

With a standard hard disk, a 100 MB primary partition is created for the Linux system and the ZENworks PBA. When the device boots, the ZENworks PBA login is displayed. After the user enters valid credentials (see [Section 1.3, “Authentication Methods,” on page 10](#)), the PBA terminates, the Windows operating system is booted, and the encrypted drives become accessible.

1.2.2 Self-Encrypting Hard Disk

A self-encrypting hard disk does its own encryption through the use of a dedicated encryption chip. It cannot be encrypted by ZENworks 11 Full Disk Encryption, but the ZENworks PBA can be used to provide extra security for the disk.

With a self-encrypting disk, a Linux system and ZENworks PBA are installed to the MBR shadow, which is a protected partition of the hard disk. When the device boots, the ZENworks PBA login is displayed. At this time, the MBR shadow is visible to the system but the Windows partition (with the self-encrypted drive) is not. After the user enters valid credentials (see [Section 1.3, “Authentication Methods,” on page 10](#)), the ZENworks PBA terminates, the Windows partition is unlocked, the Windows operating system is booted, and the encrypted drive becomes accessible.

1.3 Authentication Methods

The ZENworks PBA supports the following authentication methods:

- ◆ Standard user ID/password authentication
- ◆ Smart card authentication based on the X.509, PKCS#11, and PC/SC standards

Both methods support the user capturing and single sign-on functionality discussed in the next two sections.

- ◆ [Section 1.3.1, “User Capturing,” on page 10](#)
- ◆ [Section 1.3.2, “Single Sign-On,” on page 10](#)

1.3.1 User Capturing

A user’s credentials (either user ID/password or smart card) must be added to the ZENworks PBA. You can add credentials via the Disk Encryption policy applied to the device, or you can enable the credentials to be captured by the ZENworks PBA the first time it starts after installation. This second method, referred to as *user capturing*, is the recommended method, especially when using smart card authentication, because it increases the accuracy of correctly defining the user’s credentials.

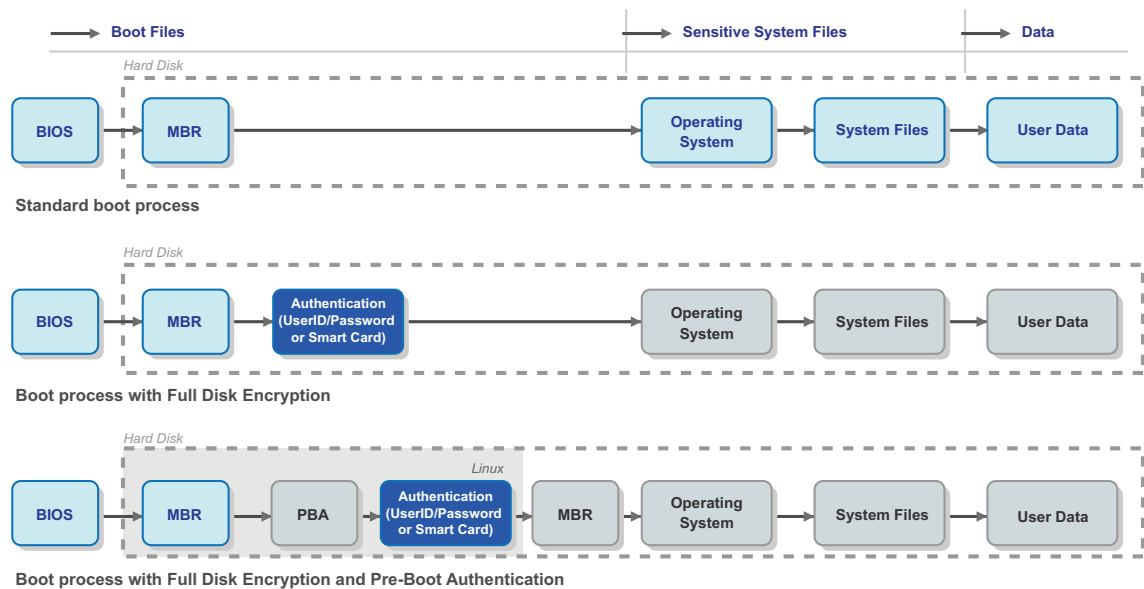
1.3.2 Single Sign-On

The ZENworks PBA login does not replace the Windows login. A user must log in to the ZENworks PBA and in to Windows. You can, however, enable single sign-on so that the user only enters credentials during the ZENworks PBA login and is automatically logged in to Windows with those same credentials. This requires that the ZENworks PBA credentials match the Windows credentials.

2 The ZENworks PBA Boot Process

When the ZENworks PBA is installed, it changes the standard boot process. The following illustration shows the standard boot process (no disk encryption or pre-boot authentication), the boot process with disk encryption (no pre-boot authentication), and the boot process with disk encryption and pre-boot authentication.

The gray boxes represent protected components and data and the light blue boxes represent unprotected components and data.



Standard Boot Process

The standard Windows boot process provides no data protection. The Windows login can be easily broken or the drive can be removed and installed as a secondary drive on another device to gain access to the data.

Boot Process With Full Disk Encryption

With full disk encryption applied to a device, the drive data is encrypted, and thus protected, until successful authentication to Windows occurs. The drive data cannot be accessed by removing the drive and installing it as a secondary drive on another device. The primary security weakness is the Windows login.

Boot Process with Full Disk Encryption and Pre-Boot Authentication

With full disk encryption and pre-boot authentication applied to a device, the drive data is encrypted until successful authentication to the ZENworks PBA occurs. This eliminates the Windows login as the key component to gaining access to the encrypted drives.

To protect the ZENworks PBA, the PBA's Linux system includes only the components needed to complete the secure authentication. The system includes no networking components. USB and CD drivers are enabled to provide emergency recovery of the device if necessary. All ZENworks PBA components are protected against manipulation.

If the device is using self-encrypting drives, the ZENworks PBA provides additional protection by locking the drive when the device shuts down. This means that the drive is completely hidden and the data is inaccessible. If the drive is connected as a secondary drive on another device, it remains hidden. The only way to unlock the drive is to provide valid authentication through the ZENworks PBA.

|| PBA Management

The following sections help you manage ZENworks Pre-Boot Authentication:

- ♦ [Chapter 3, “Activating Pre-Boot Authentication,” on page 15](#)
- ♦ [Chapter 4, “Enabling User Capturing,” on page 17](#)
- ♦ [Chapter 5, “Manually Adding Users,” on page 21](#)
- ♦ [Chapter 6, “Enabling Single Sign-On with Windows,” on page 25](#)
- ♦ [Chapter 7, “Synchronizing PBA and Windows Credentials,” on page 29](#)

3 Activating Pre-Boot Authentication

ZENworks Pre-Boot Authentication is activated on a device by deploying a Disk Encryption policy to the device. The policy also defines the supported authentication methods (user ID/password or smart card) for the device and enables options such as user capturing and single sign-on.

Creation and deployment of Disk Encryption policies is covered in the [ZENworks 11 SP2 Full Disk Encryption Policy Reference](#).

4 Enabling User Capturing

The ZENworks PBA can be enabled to capture the credentials (user ID/password or smart card) of the next user who logs in to the device. This process is referred to as *user capturing*.

If a Disk Encryption policy has user capturing enabled, the ZENworks PBA captures the credentials of the first user to log in after the policy is applied. You can also enable user capturing after the policy is applied through a ZENworks Control Center Quick Task or through the ZENworks Full Disk Encryption Agent. After user capturing is enabled, the ZENworks PBA captures the credentials of the next user to log in and adds them to any other captured credentials.

The following sections cover both methods of enabling user capturing:

- ♦ [Section 4.1, “Using a ZENworks Control Center Quick Task,” on page 17](#)
- ♦ [Section 4.2, “Using the Full Disk Encryption Agent,” on page 18](#)

4.1 Using a ZENworks Control Center Quick Task

To use a ZENworks Full Disk Encryption Quick Task in ZENworks Control Center, a ZENworks administrator must be assigned the *Manage Endpoint Security Settings and Tasks* privilege. This privilege is configured through the Quick Tasks rights for administrators and administrator groups. For help configuring Quick Tasks rights, see [“Managing Administrators and Administrator Groups”](#) in the *ZENworks 11 SP2 ZENworks Control Center Reference*.

For user capturing to be enabled on a device through a Quick Task, the device must be running and have a network connection to the ZENworks Server. Otherwise, the ZENworks Server cannot deliver the Quick Task to the device.

- 1 In ZENworks Control Center, click *Devices*.
- 2 In the *Devices* panel, locate the device for which you want to enable user capturing.
- 3 Select the check box next to the device, click *Quick Tasks*, click *FDE: Enable Additive User Capturing*, then click *OK* to confirm the task.
- 4 In the Quick Task Status dialog box, click *Start* if you want to use the default options.

or

Configure the options as desired, then click *Start*.


For information about the options, click the Help icon in the Quick Task Status dialog box.

- 5 As soon as the Quick Task is complete, have the user restart the device.

Until the device restarts and the correct user’s credentials are captured, the device’s security is compromised. Having the user immediately restart the device minimizes this possible security threat.

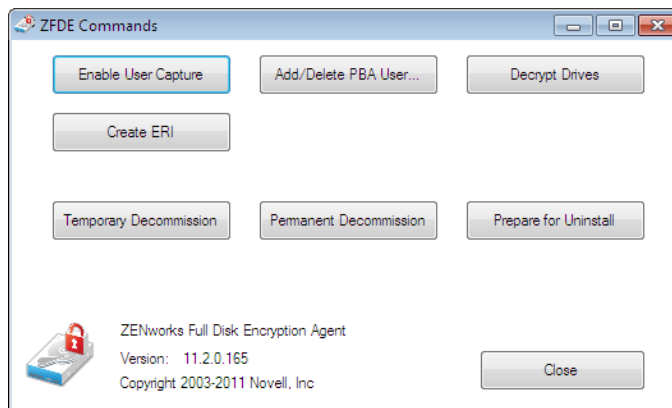
4.2 Using the Full Disk Encryption Agent

To use the ZENworks Full Disk Encryption Agent to enable user capturing on a device, you must know the FDE Administrator password for the policy assigned to the device, or you must know the ZENworks Adaptive Agent override password or key.

- 1 On the device, double-click the  icon in the notification area, then click *Full Disk Encryption*.
- 2 In the *Full Disk Encryption Agent Actions* section, click *About* to display the About dialog box.



- 3 Click the *Commands* button.
- 4 Supply the password to display the Commands dialog box.



- 5 Click the *Enable User Capture* button.

You can verify the setting by viewing the agent status (in the About dialog box) and looking at the *PBA Self Initialization Mode* value. If user capturing is enabled, the value is `WINDOWS_CRED_SELFINIT`.

6 Exit the Full Disk Encryption Agent and restart the device.

Until the device restarts and the correct user's credentials are captured, the device's security is compromised. Immediately restarting the device minimizes this possible security threat.

5 Manually Adding Users

In addition to having the ZENworks PBA automatically capture users (see [Chapter 4, “Enabling User Capturing,” on page 17](#)), you can manually add users to the ZENworks PBA for a device. You cannot manually add smart cards.

As with captured users, users that you manually add exist only on the device; they are not added to the Disk Encryption policy’s user list. Therefore, if the *Remove existing users from PBA if not in this list* option is enabled in the Disk Encryption policy, the added user is removed after the next login.

You can add users through a ZENworks Control Center Quick Task or through the ZENworks Full Disk Encryption Agent. The following sections cover both methods:

- ♦ [Section 5.1, “Using a ZENworks Control Center Quick Task,” on page 21](#)
- ♦ [Section 5.2, “Using the Full Disk Encryption Agent,” on page 22](#)

5.1 Using a ZENworks Control Center Quick Task

To use a ZENworks Full Disk Encryption Quick Task in ZENworks Control Center, a ZENworks administrator must be assigned the *Manage Endpoint Security Settings and Tasks* privilege. This privilege is configured through the Quick Tasks rights for administrators and administrator groups. For help configuring Quick Tasks rights, see [“Managing Administrators and Administrator Groups”](#) in the *ZENworks 11 SP2 ZENworks Control Center Reference*.

For a user to be added to a device through a Quick Task, the device must be running and have a network connection to the ZENworks Server. Otherwise, the ZENworks Server cannot deliver the Quick Task to the device.

- 1 In ZENworks Control Center, click *Devices*.
- 2 In the *Devices* panel, locate the device for which you want to add a user.
- 3 Select the check box next to the device, click *Quick Tasks > FDE: Update PBA User* to display the Update PBA User dialog box.
- 4 Fill in the following fields:

Replace password if user already exists in PBA: Ignore this option. It only applies if you are updating an existing user’s password.

User Name: Specify a user name for the PBA user. If single sign-on is active on the device, this user name must be the same as the Windows user name. If single sign-on is not active, the user name does not need to match the Windows user name.

Domain: Specify a domain name for the PBA user. If single sign-on is active, this must be the Windows domain name (or computer name if the user is not a domain member). If single sign-on is not active, this field is optional. You can leave it blank or use it as another component to distinguish the PBA user name.


Password: Specify a password for the PBA user. If single sign-on is active, this must be the Windows password. If single sign-on is not active, you can specify any password.

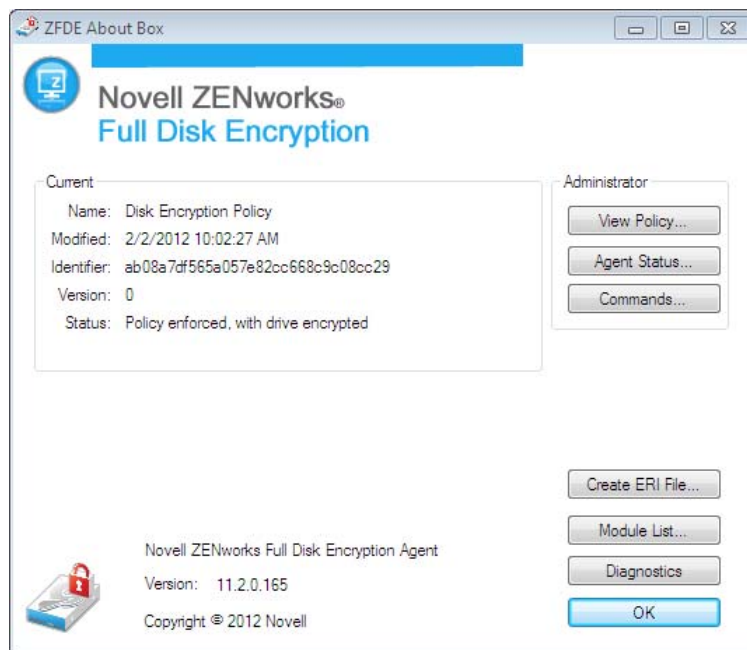
- 5 Click *OK* to display the Quick Task Status dialog box.
- 6 In the Quick Task Status dialog box, click *Start* if you want to use the default options.
or
Configure the options as desired, then click *Start*.
For information about the options, click the Help icon in the Quick Task Status dialog box.
As soon as the Quick Task is complete, the new user can authenticate to the ZENworks PBA on the device.

5.2 Using the Full Disk Encryption Agent

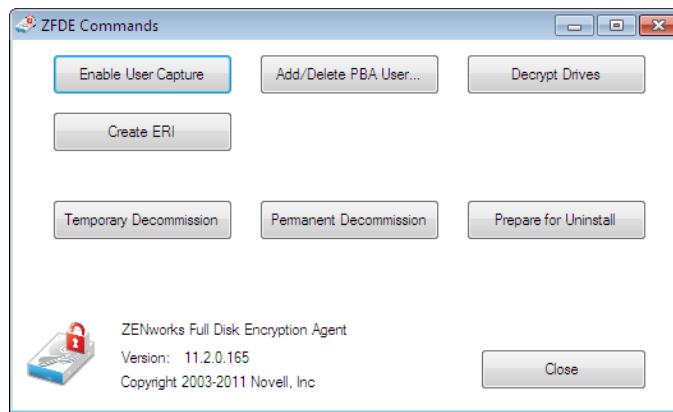
You can use the Full Disk Encryption Agent to add users to or remove users from the ZENworks PBA.

To add or remove a PBA user, you must know the FDE Administrator password for the policy assigned to the device, or you must know the ZENworks Adaptive Agent override password or key.

- 1 On the device, double-click the  icon in the notification area, then click *Full Disk Encryption*.
- 2 In the *Full Disk Encryption Agent Actions* section, click *About* to display the About dialog box.



- 3 Click the *Commands* button.
- 4 Supply the password, then click *OK* to display the Commands dialog box.



5 Click the *Add/Delete PBA User* button.

6 Provide the username, password, and domain of the user you want to add or delete.

User Name: Specify a user name for the PBA user. If single sign-on is active on the device, this user name must be the same as the Windows user name. If single sign-on is not active, the user name does not need to match the Windows user name.

User Password: Specify a password for the PBA user. If single sign-on is active, this must be the Windows password. If single sign-on is not active, you can specify any password.

User Domain: Specify a domain name for the PBA user. If single sign-on is active, this must be the Windows domain name (or computer name if the user is not a domain member). If single sign-on is not active, this field is optional. You can leave it blank or use it as another component to distinguish the PBA user name.

7 (Conditional) If you want to delete the user, select the *Check to Delete User* box.

8 Click *OK* to add or delete the user.

You can verify the change by viewing the agent status and looking at the *PBA User List*.

6 Enabling Single Sign-On with Windows

Users authenticate to both the ZENworks PBA and the Windows operating system. You can enable single sign-on so that the user logs in to the ZENworks PBA and the PBA handles the login to the Windows operating system. This, of course, requires that the user's PBA and Windows credentials are the same. Single sign-on applies to both authentication methods (user ID/password or smart card).

If you are using ZENworks login to enable policies and bundles to be applied to users as well as devices, and you have configured ZENworks login for single sign-on with your Windows login, single sign-on works for all three logins. When a user logs in to the ZENworks PBA, the credentials are passed to the Windows login and then the ZENworks login.

Complete the following sections to enable single sign-on:

- ♦ [Section 6.1, "Activating Single Sign-On in the Disk Encryption Policy," on page 25](#)
- ♦ [Section 6.2, "Configuring Windows Login," on page 26](#)
- ♦ [Section 6.3, "Using the Novell Client," on page 27](#)

6.1 Activating Single Sign-On in the Disk Encryption Policy

Single sign-on is activated through the Disk Encryption policy assigned to a device:

- ♦ To create a new policy and assign it to a device, see ["Policy Deployment"](#) in the *ZENworks 11 SP2 Full Disk Encryption Policy Reference*.
- ♦ To modify an existing policy and republish it to a device, see ["Policy Management"](#) in the *ZENworks 11 SP2 Full Disk Encryption Policy Reference*.

6.2 Configuring Windows Login

Single sign-on supports both the classic Logon screen mode (left screen shot) and the Welcome screen mode (right screen shot). As long as a device is using one of these two modes, single sign-on works as soon it is activated in the policy and the policy is applied to the device. Windows 7 is used in the example screen shots below, but Windows Vista and Windows XP also provide the classic Logon screen and Welcome screen modes.



Single sign-on also supports Secure Logon (shown below) in both of these modes. However, as with the standard Windows login process, the user must press Ctrl+Alt+Delete to dismiss the Secure Logon screen before the single sign-on process can continue.



If single sign-on is failing on a device, we recommend that you set the device to use the classic Logon screen without Secure Logon. In addition, we recommend that you set the *Do Not Display Last User Name* option to Enabled so that the Logon screen is not automatically populated with the user name of the last person to successfully log in.

To configure these settings locally on a Windows XP device:

- 1 Log on to the device as an administrator.
- 2 Set classic Logon screen mode:
 - 2a Click the *Start* menu, click *Run*, type `gpedit.msc`, then click *OK* to open the Local Group Policy Editor.
 - 2b In the editor, expand *Local Computer Policy* > *Computer Configuration* > *Administrative Templates* > *System* > *Logon*.

- 2c Double-click *Always Use Classic Logon*.
- 2d Select *Enabled*, then click *OK*.
- 3 Disable Secure Logon:
 - 3a Click the *Start* menu, click *Run*, type `control userpasswords2`, then click *OK* to open the User Accounts dialog box.
 - 3b Click the *Advanced* tab.
 - 3c In the Secure logon section, deselect *Require users to press Ctrl+Alt+Delete*.
 - 3d Click *OK*.
- 4 Enable the Do Not Display Last User Name setting:
 - 4a Click the *Start* menu, click *Run*, type `secpol.msc`, then click *OK* to open the Local Security Settings.
 - 4b Expand *Local Policies > Security Options*.
 - 4c Double-click *Interactive logon: Do not display last user name*.
 - 4d Select *Enabled*, then click *OK*.

To configure these settings locally on a Windows Vista or Windows 7 device:

- 1 Log on to the device as an administrator.
- 2 Set classic Logon screen mode:
 - 2a Click the *Start* menu, type `gpedit.msc` in the search box, then click *OK* to open the Local Group Policy Editor.
 - 2b In the editor, expand *Local Computer Policy > Computer Configuration > Administrative Templates > System > Logon*.
 - 2c Double-click *Always Use Classic Logon*.
 - 2d Select *Enabled*, then click *OK*.
- 3 Disable Secure Logon:
 - 3a Click the *Start* menu, type `netplwiz` in the search box, then click *OK* to open the User Accounts dialog box.
 - 3b Click the *Advanced* tab.
 - 3c In the Secure logon section, deselect *Require users to press Ctrl+Alt+Delete*.
 - 3d Click *OK*.
- 4 Enable the Do Not Display Last User Name setting:
 - 4a Click the *Start* menu, click *Run*, type `secpol.msc`, then click *OK* to open the Local Security Settings.
 - 4b Expand *Local Policies > Security Options*.
 - 4c Double-click *Interactive logon: Do not display last user name*.
 - 4d Select *Enabled*, then click *OK*.

6.3 Using the Novell Client

If a device is using the Novell Client for Windows login, be aware of the following requirements:

- ♦ Novell Client 2 SP2 IR1 is recommended on Windows 7 and Windows Vista.

- ♦ When using user ID/password authentication with the Novell Client and DLU, the user needs to log in to the Novell Client once before single sign-on will work. During single sign-on, the ZENworks PBA passes the user ID and password to the Novell Client. However, the client requires other details (tree, server, context, and so forth) that are available only if the user has populated the details during a previous log in.
- ♦ When using smart card authentication with the Novell Client, NESCM (Novell Enhanced Smart Card Method), and DLU, the user needs to be the last user to have logged in to the Novell Client. During single sign-on, the ZENworks PBA passes the pin to the Novell Client. However, the client requires other details (tree, server, context, and so forth) that are available only if the user was the last smart card user to log in to the client.
- ♦ Smart card authentication with the Novell Client, NESCM, and *Disconnected Workstation Only* mode is not supported.

7 Synchronizing PBA and Windows Credentials

If a device's Disk Encryption policy has single sign-on enabled so that the ZENworks PBA login credentials are the same as the Windows login credentials, the passwords remain synchronized as long as the Windows password is changed through one of the following methods:

- ♦ Via Windows domain login
- ♦ Via Windows local login
- ♦ Using Ctrl+Alt+Del to access the change password feature

The passwords are not synchronized if one of the following methods is used:

- ♦ Control Panel
- ♦ Device Manager

If the passwords become out-of-sync, the following methods can be used to synchronize them while at the device:

- ♦ [Section 7.1, "Using the Windows Login," on page 29](#)
- ♦ [Section 7.2, "Using a ZENworks Control Center Quick Task," on page 30](#)
- ♦ [Section 7.3, "Using the Full Disk Encryption Agent," on page 30](#)

7.1 Using the Windows Login

This is the recommended way to synchronize a user's PBA and Windows passwords because the user can complete these steps without administrator assistance:

- 1 Restart the device.
- 2 Log in to the ZENworks PBA using the old Windows/PBA password.
- 3 When the Windows login screen is displayed, enter the password required to log in to Windows.
The ZENworks PBA detects the difference in the current PBA and Windows passwords and changes the PBA password to the Windows password.
- 4 Restart the device and log in to the ZENworks PBA using the new Window/PBA password.

7.2 Using a ZENworks Control Center Quick Task

To use a ZENworks Full Disk Encryption Quick Task in ZENworks Control Center, a ZENworks administrator must be assigned the *Manage Endpoint Security Settings and Tasks* privilege. This privilege is configured through the Quick Tasks rights for administrators and administrator groups. For help configuring Quick Tasks rights, see “[Managing Administrators and Administrator Groups](#)” in the *ZENworks 11 SP2 ZENworks Control Center Reference*.

Using a Quick Task to synchronize a user’s PBA password with his or her Windows password requires you to know the Windows password.

- 1 In ZENworks Control Center, click *Devices*.
- 2 In the *Devices* panel, locate the user’s device.
- 3 Select the check box next to the device, then click *Quick Tasks > FDE: Update PBA User* to display the Update PBA User dialog box.
- 4 Fill in the following fields:
 - Replace password if user already exists in PBA:** Make sure this option is selected.
 - User Name:** Specify the Windows user name.
 - Domain:** Specify the user’s Windows domain name. If the user is not a member of a domain, you can specify the computer name or leave the field blank.
 - Password:** Specify the user’s Windows password.
- 5 Click *OK* to display the Quick Task Status dialog box.
- 6 In the Quick Task Status dialog box, click *Start* if you want to use the default options.

or

Configure the options as desired, then click *Start*.


For information about the options, click the Help icon in the Quick Task Status dialog box.

As soon as the Quick Task is complete, the user can authenticate to the ZENworks PBA using the new password.

7.3 Using the Full Disk Encryption Agent

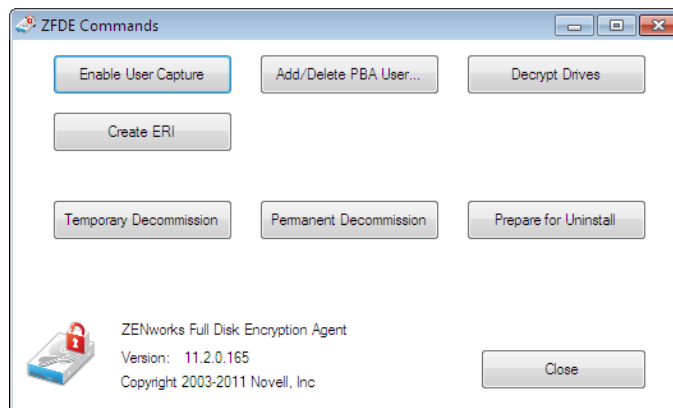
You can use the Full Disk Encryption Agent to change the user’s PBA password to match the Windows password.

To change the user’s PBA password, you must know the FDE Administrator password for the policy assigned to the device, or you must know the ZENworks Adaptive Agent override password or key.

- 1 On the device, double-click the  icon in the notification area, then click *Full Disk Encryption*.
- 2 In the *Full Disk Encryption Agent Actions* section, click *About* to display the About dialog box.



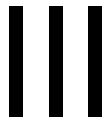
- 3 Click the *Commands* button.
- 4 Supply the password, then click *OK* to display the Commands dialog box.



- 5 Click the *Add/Delete PBA User* button.
- 6 Provide the following:
 - User Name:** Specify the user name for the user whose password you want to change.
 - User Password:** Specify the user's Windows password. This becomes the PBA password.
 - User Domain:** Specify the user's Windows domain name. If the user is not a member of a domain, you can specify the computer name or leave the field blank.

If you don't know the domain or computer name, you can cancel to exit the dialog box, close the Commands dialog box, click the *Agent Status* button, click the *PBA* tab, then scroll down to the *User List* at the bottom of the page. The user name and domain/computer name are listed in the *PBA User Name* column, with the domain/computer name listed second (after the colon).

- 7 Click *OK* to change the PBA password.



PBA Override

The following sections provides information about overriding ZENworks Pre-Boot Authentication in cases such as a forgotten password or lost smart card:

- ♦ [Chapter 8, “PBA Override Versus Emergency Recovery,” on page 35](#)
- ♦ [Chapter 9, “Using the ZENworks PBA Helpdesk for PBA Override \(User\),” on page 37](#)
- ♦ [Chapter 10, “Generating a Response Sequence for PBA Override \(Administrator\),” on page 41](#)
- ♦ [Chapter 11, “Overriding the PBA with an ERI File,” on page 47](#)

8 PBA Override Versus Emergency Recovery

ZENworks Full Disk Encryption provides both authentication override for ZENworks Pre-Boot Authentication and emergency recovery of devices and their encrypted hard disks.

Pre-Boot Authentication Override (or PBA Override) is used in situations where the ZENworks PBA is still functional but the user cannot authenticate for reasons such as:

- ♦ The PBA credential (user ID/password) is forgotten.
- ♦ The smart card reader is defective.
- ♦ The smart card is lost or broken.
- ♦ The smart card PIN is forgotten or blocked.
- ♦ The PBA lockout has been invoked because of too many failed logins.

PBA Override cannot be used in the following situations. Instead, you need to perform an emergency recovery:

- ♦ The device does not start correctly or does not present the user with the ZENworks PBA login or the Windows login.
- ♦ Windows login is being used as the authentication method (no ZENworks PBA) and the Windows credentials have been forgotten or the user's smart card has been lost or damaged.
- ♦ ZENworks Full Disk Encryption has been removed from the device but the hard disk is still encrypted.

This *ZENworks 11 Full Disk Encryption Pre-Boot Authentication Reference* does not provide information about emergency recovery. For information about emergency recovery, see the [ZENworks 11 SP2 Full Disk Encryption Emergency Recovery Reference](#).

9 Using the ZENworks PBA Helpdesk for PBA Override (User)

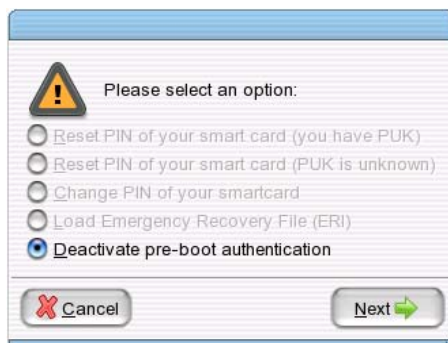
PBA Override uses the *challenge-response* methodology. The device user must provide a ZENworks administrator with a *request ID* and *challenge sequence* that can be used to generate a *response sequence* in ZENworks Control Center. When the response sequence is entered at the device, it authorizes the user to bypass the PBA for a set number of times.

The following steps explain how to use the ZENworks PBA Helpdesk to override the PBA. The steps must be performed on the device where the override is required. In addition, the ZENworks administrator must perform the steps in [Chapter 10, “Generating a Response Sequence for PBA Override \(Administrator\),” on page 41](#) to provide the user with the required response sequence.

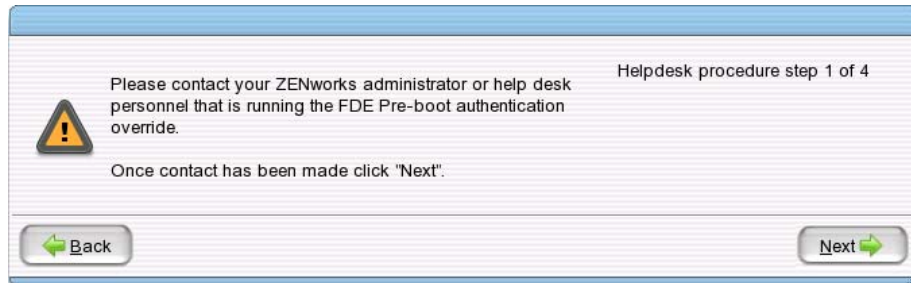
- 1 Start the device so that it boots to the ZENworks PBA login screen.



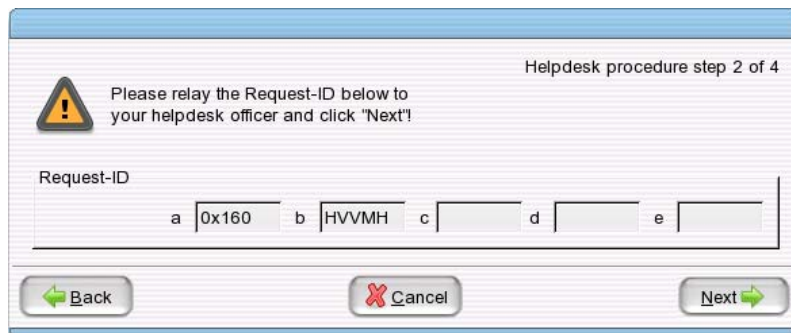
- 2 Click *Helpdesk*.



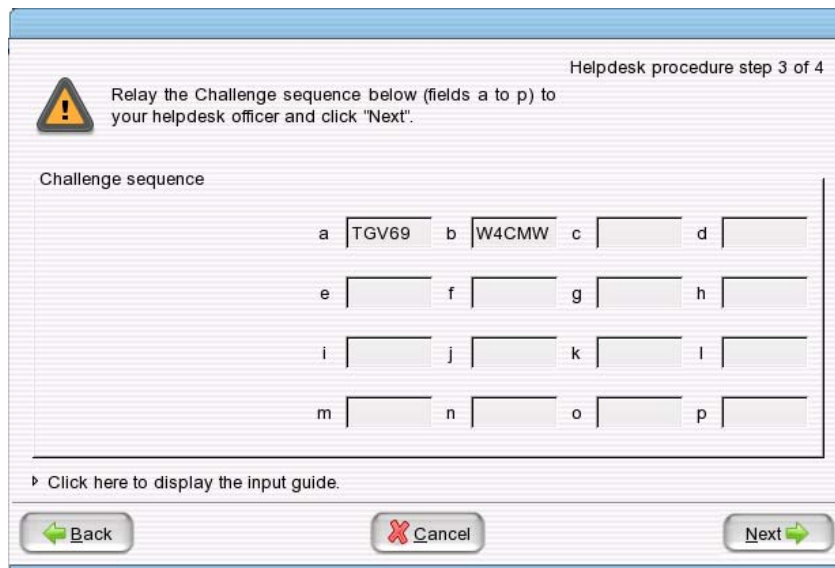
- 3 Make sure that *Deactivate pre-boot authentication* is selected, then click *Next*.



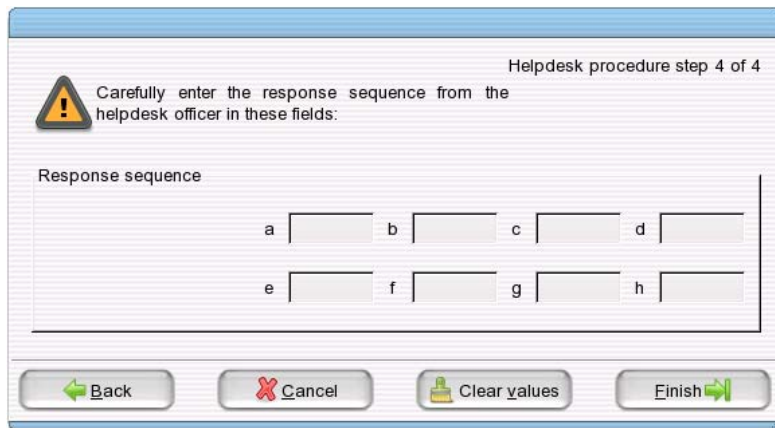
- 4 Contact your ZENworks administrator, then click *Next* to display the Request ID dialog box.



- 5 Give the request ID to your ZENworks administrator, then click *Next* to display the Challenge Sequence dialog box.



- 6 Give the challenge sequence to your ZENworks administrator, then click *Next* to display the Response Sequence dialog box.



Helpdesk procedure step 4 of 4

Carefully enter the response sequence from the helpdesk officer in these fields:

Response sequence

a b c d

e f g h

Back Cancel Clear values Finish

- 7 Enter the response sequence you receive from your ZENworks administrator.
If you enter a value incorrectly, the box is outlined in red. Enter the value again before proceeding with the next value.
- 8 Click *Finish*.
The device boots to Windows.

10 Generating a Response Sequence for PBA Override (Administrator)

PBA Override uses the *challenge-response* methodology. The user provides you with a *request ID* and *challenge sequence* that you use to generate a *response sequence* in ZENworks Control Center. You then provide the user with the response sequence that authorizes the user to bypass the PBA for a set number of times.

By default, the response sequence is calculated by using the Management Zone's unique override key. Therefore, it works only with devices registered in the zone. If you need to generate a response for a device registered in another zone, you must export a PBA Override file from that zone and use the PBA Override file to generate the correct response. The following sections provide instructions for both methods:

- ♦ [Section 10.1, "Assigning the Administrator Rights Needed for PBA Override,"](#) on page 41
- ♦ [Section 10.2, "Generating a Response with the Zone Key,"](#) on page 43
- ♦ [Section 10.3, "Generating a Response with a PBA Override File,"](#) on page 44

10.1 Assigning the Administrator Rights Needed for PBA Override

Super Administrators have rights to perform all tasks in ZENworks Control Center. If a ZENworks administrator is not a Super Administrator, the administrator must be assigned the *Manage FDE PBA Override* privilege to use the PBA Override feature. If the administrator does not have this privilege, he or she is restricted to view rights for the PBA Override page.

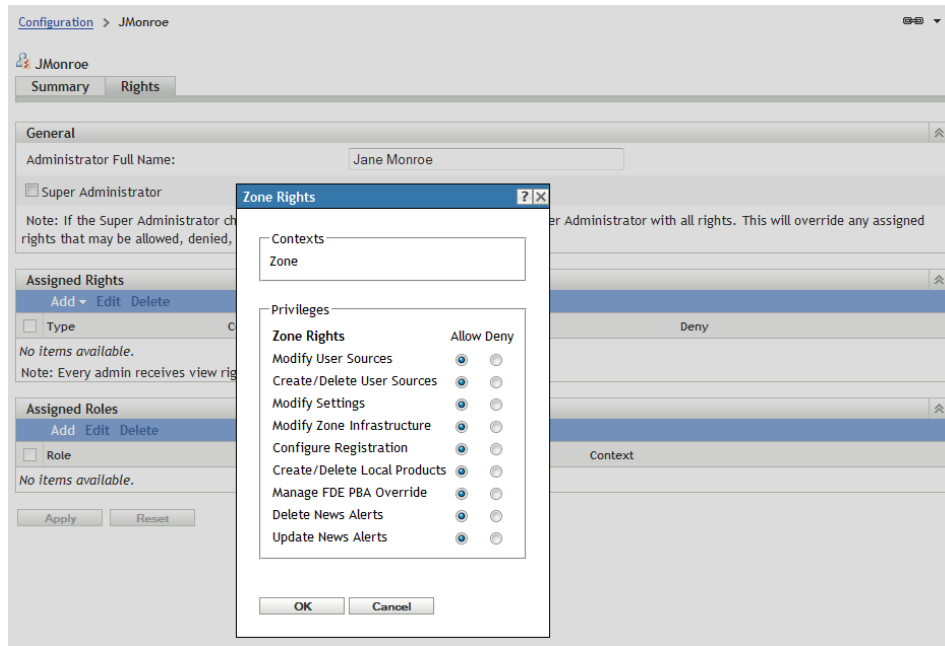
This *Manage FDE PBA Override* privilege is configured through the Zone rights for individual administrators or administrator groups.

- 1 In ZENworks Control Center, click *Configuration*.
- 2 In the Administrators panel, click the administrator or administrator group to which you want to assign the privilege.

You can also use roles to assign the privilege to administrators. For instructions, see "[Managing Administrator Roles](#)" in the *ZENworks 11 SP2 ZENworks Control Center Reference*.

- 3 Click the *Rights* tab.

- 4 In the Assigned Rights panel, click *Add > Zone Rights* to display the Zone Rights dialog box.



- 5 By default, all privileges are set to *Allow*. Change any privileges you don't want the administrator to have to *Deny*, then click *OK*.
- 6 Click *Apply* to apply the changes to the administrator.

10.2 Generating a Response with the Zone Key

- 1 In ZENworks Control Center, click *Full Disk Encryption*, then click *Pre-Boot Authentication Override*.

The screenshot shows the 'Pre-Boot Authentication Override' configuration page. At the top, there are three tabs: 'Workflow', 'Pre-Boot Authentication Override' (which is selected), and 'Emergency Recovery'. Below the tabs, there is a descriptive paragraph about PBA Override. The main form contains several sections: 'Request ID' with two input fields labeled 'a' and 'b'; 'Challenge' with two input fields labeled 'a' and 'b'; 'Overrides Allowed' with a label 'Number of PBA overrides allowed: *' and an input field containing the number '1'. Below these sections are two buttons: 'Generate Response' and 'Clear Values'. The 'Response' section is a large empty text area. The 'PBA Override File' section includes a checkbox 'Use PBA Override file to generate response', a label 'PBA Override File:' with an input field, and a label 'PBA Override File Password:' with an input field.

- 2 In the *Request ID* fields, specify the request ID sequence supplied to you by the user.
The request ID sequence must be identical to the sequence presented to the user on his or her device. Your *Request ID* field A corresponds directly to the user's *Request ID* field A and your *Request ID* field B corresponds to the user's *Request ID* field B. Incorrect characters or order cause a sequence mismatch, resulting in an error when generating the response sequence.
- 3 In the *Challenge* fields, specify the challenge sequence supplied to you by the user.
As with the request ID sequence, the challenge sequence you enter must exactly match (characters and order) the user's challenge sequence.
- 4 In the *Overrides Allowed* field, specify the number of times you want to allow the user to boot the device without providing PBA authentication.
- 5 Click *Generate Response*.
- 6 Supply the response sequence to the user.
As with the request ID and challenge sequences you entered earlier, the user must enter the response sequence to exactly match (characters and order) the generated response sequence.

10.3 Generating a Response with a PBA Override File

The following instructions assume that you have exported the PBA Override file from another zone and want to use it to create a response for a device from that zone. The PBA Override file contains the override key from the other zone, which is needed to create the correct response for that zone's devices.

To generate a response:

- 1 In ZENworks Control Center, click *Full Disk Encryption*, then click *Pre-Boot Authentication Override*.

The screenshot shows the 'Pre-Boot Authentication Override' configuration page in ZENworks Control Center. At the top, there are three tabs: 'Workflow', 'Pre-Boot Authentication Override' (which is selected), and 'Emergency Recovery'. Below the tabs, there is a descriptive paragraph: 'Pre-Boot Authentication (PBA) Override helps a user boot a device in the event of an emergency such as a forgotten password or lost smart card. PBA Override uses the challenge-response methodology. The user provides you with a request ID and challenge sequence generated by the PBA on the user's device. You enter the data and specify the number of overrides you want to allow, then generate the response and provide it to the user. The response is calculated using the zone's unique override key.'

The form contains several sections:

- Request ID ***: Two input fields labeled 'a' and 'b' for entering the request ID sequence.
- Challenge ***: Two input fields labeled 'a' and 'b' for entering the challenge sequence.
- Overrides Allowed**: A label 'Number of PBA overrides allowed: *' followed by an input field containing the number '1'.
- Buttons**: 'Generate Response' and 'Clear Values' buttons.
- Response**: A large, empty text area for displaying the generated response.
- PBA Override File**: A section with a descriptive paragraph: 'The challenge-response requires that the device and zone have the same override key. If the device is from another zone (or for some reason has a different key), and you have a PBA Override (*.hdf) file that contains that key, you can use the PBA Override file to generate the correct response.' Below this is a checkbox labeled 'Use PBA Override file to generate response'. If checked, there are two input fields: 'PBA Override File:' and 'PBA Override File Password:'.

- 2 In the *Request ID* section, specify the request ID sequence supplied to you by the user.
The request ID sequence must be identical to the sequence presented to the user on his or her device. Your *Request ID* field A corresponds directly to the user's *Request ID* field A and your *Request ID* field B corresponds to the user's *Request ID* field B. Incorrect characters or order cause a sequence mismatch, resulting in an error when generating the response sequence.
- 3 In the *Challenge* section, specify the challenge sequence supplied to you by the user.
As with the request ID sequence, the challenge sequence you enter must exactly match (characters and order) the user's challenge sequence.
- 4 In the *Overrides Allowed* section, specify the number of times you want to allow the user to boot the device without providing PBA authentication.

- 5 In the *PBA Override File* section, select the *Use PBA Override file to generate response* option, select the PBA Override (*.hdf) file, then specify the password for the file.
- 6 Click *Generate Response*.
- 7 Supply the response sequence to the user.
As with the request ID and challenge sequences you entered earlier, the user must enter the response sequence to exactly match (characters and order) the generated response sequence.

11 Overriding the PBA with an ERI File

A device's emergency recovery information (ERI) file can be used to perform a PBA override on self-encrypting hard disks. This method does not apply to standard hard disks.

Rather than use the challenge-response methodology, a user can load the ERI file for his or her device (including the ERI password) to bypass the ZENworks PBA. The bypass can unlock the disk one time, so the PBA remains active, locks the disk the next time the device powers off, and enforces pre-boot authentication on the next start up. Or, the bypass can deactivate the PBA, so the disk remains unlocked and no pre-boot authentication takes place on subsequent device startups.

- 1 Make sure the media (for example, a USB drive) containing the ERI file is inserted in the device.
- 2 Start the device so that it boots to the ZENworks PBA login screen.



- 3 Click *Helpdesk*.



- 4 Select *Load Emergency Recovery File*, then click *Next*.
- 5 Use the file browser to locate and select the ERI file.
- 6 Choose the action you want performed when the ERI is loaded:
 - ♦ **Unlock disk temporarily:** This bypasses the PBA one time.
 - ♦ **Deactivate pre-boot authentication:** This bypasses the PBA permanently.

7 Click *OK* to display the ERI password dialog box.

8 Provide the ERI password, then click *OK*.

Pre-boot authentication is bypassed and the device boots to the Windows operating system. This process can take several minutes.